DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/23/2008 has been entered.

2. Claims 2-3, 6-10, 14 and 16-18 are cancelled. Also, claims 23-35 are withdrawn.

Response to Arguments

3. Applicant's arguments filed 10/23/2008 have been fully considered but they are not persuasive.

(1) argument 1:

Applicant argues that neither Slick et al. nor Kurishita et al. disclose "a system and a method for changing a printing mode a printing device that is to be used on future print jobs."

With respect to Applicant's argument, a system and a method for changing a printing mode a printing device that is to be used on future print jobs, Kurishita et

al. disclose a method for changing a printing mode (**column 2, lines 1-9; note that a print method for securely printing print data is disclosed**) of *a printing device that is to be used on future print jobs* (**column 2, lines 18-19; note that the method is used to print job or data in a printing device**). Thus, the stated argument is taught by Kurishita et al. Slick et al. and Kurishita et al. are combinable because they are from the same field of endeavor i.e. network printing. The suggestion/motivation for doing so would have been to have a reliable and secure print system such that a user having issues a print request can reliably obtain printouts while observing secrecy (column 1, lines 7-10). Therefore, it would have been obvious to combine Slick et al. and Kurishita et al. to obtain the invention as specified in the argument.

(2) argument 2:

Applicant argues that neither Slick et al. nor Kurishita et al. disclose generating a signed request that requests changing of the printing mode that will be used for print jobs that are received by the printing device or printing the signed request to the printing device independent of a print job.

With respect to Applicant's argument, generating a signed request that requests changing of the printing mode that will be used for print jobs that are received by the printing device or printing the signed request to the printing device independent of a print job, generating a signed request that requests changing of

the printing mode (**column 6, lines 11-17; note that there is a generated user information for authenticating the print data)** *that will be used for print jobs that are received by the printing device* (**column 6, lines 4-8; note that the user goes to the printer and operated the input operation or the printing operation**); providing the signed request to the printing device *independent of a print job* (**column 6, lines 11-17; note that user inputs user name as a signed request. Also, in lines 26-30; note that the signed request is verified independent of a print job**). Thus, the stated argument is taught by Kurishita et al. Slick et al. and Kurishita et al. are combinable because they are from the same field of endeavor i.e. network printing. The suggestion/motivation for doing so would have been to have a reliable and secure print system such that a user having issues a print request can reliably obtain printouts while observing secrecy (column 1, lines 7-10). Therefore, it would have been obvious to combine Slick et al. and Kurishita et al. to obtain the invention as specified in the argument.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 4-5, 13, 15, 20-22 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slick et al. (US Patent Number 7,111,322 B2) in view of Kurishita et al. (US Patent Number 7,100,198 B2).

(1) regarding claim 1:

As shown in figure 10A, Slick et al. discloses generating a digital signature by encrypting with a private key control information **(column 1, lines 29-30; note that private key is generally maintained within the printer and in column 2, lines 38-41, it is stated that a key is encrypted within the printer itself. Also, in column 16, lines 39-42, the key used is a digital signature**); the signed request including the digital signature **(column 16, lines 40-42; note that the key is used to apply a digital signature to the signed hash fields)**; decrypting with a public key associated with the private key the digital signature to obtain decrypted control information **(column 1, line 65-column 2, lines 4; note that the validated key gets checked on the public key by performing a hashing algorithm over the key. Also, the network device utilizes a corresponding encryption key of the new encryption keypair to decrypt the encrypted print job**); and the printing device comparing the decrypted control information with other information to determine if they match **(column 11, lines 61-66; note that the encrypted key is checked to match an expected value**), a match indicating that the signed request is valid **(column 2, lines 42-44; note that the key i.e. digital signature as described in column 16, lines 39-42, gets validated**);

Slick et al. disclose all of the subject matter as described as above except for specifically teaching a method for changing a printing mode of *a printing device that is to be used on future print jobs*; receiving a request to change a printing mode of the printing device; generating a signed request that requests changing of the printing mode *that will be used for print jobs that are received by the printing device*; providing the signed request to the printing device *independent of a print job*; the printing device validating the signed request; and the printing device *changing* the printing mode in accordance with the signed request if the signed request is valid.

However, As shown in figures 4-5, Kurishita et al. disclose a method for changing a printing mode (**column 2, lines 1-9; note that a print method for securely printing print data is disclosed**) of *a printing device that is to be used on future print jobs (***column 2, lines 18-19; note that the method is used to print job or data in a printing device***)*, the method comprising: receiving a request to change a printing mode of a printing device (**column 5, lines 30-34; note that the printing device receives instruction from the host computer**); generating a signed request that requests changing of the printing mode (**column 6, lines 11-17; note that there is a generated user information for authenticating the print data**) *that will be used for print jobs that are received by the printing device (***column 6, lines 4-8; note that the user goes to the printer and operated the input operation or the printing operation***)*; providing the signed request to the printing device *independent of a print job* (**column 6, lines 11-17; note that user inputs user name as a signed request. Also, in lines 26-30; note that the signed request is verified independent of a print job**); the printing device

validating the signed request (**column 6, lines 18-25; note that based upon the requestors input i.e. user name selected, the user gets validated or authorized**); and the printing device changing the printing mode in accordance with the signed request if the signed request is valid (**column 6, lines 26-32; note that if the data entered in valid, the print data stored is transmitted to be printed or executed**).

Slick et al. and Kurishita et al. are combinable because they are from the same field of endeavor i.e. network printing. At the time of the invention, it would have been obvious to a person of ordinary skilled in the art to method for changing a printing mode of *a printing device that is to be used on future print jobs*; receiving a request to change a printing mode of the printing device; generating a signed request that requests changing of the printing mode *that will be used for print jobs that are received by the printing device*; providing the signed request to the printing device *independent of a print job*; the printing device validating the signed request; and the printing device *changing* the printing mode in accordance with the signed request if the signed request is valid. The suggestion/motivation for doing so would have been to have a reliable and secure print system such that a user having issues a print request can reliably obtain printouts while observing secrecy (column 1, lines 7-10). Therefore, it would have been obvious to combine Slick et al. and Kurishita et al. to obtain the invention as specified in claim 1.

(2) regarding claim 4:

Slick et al. further disclose the method of claim 1, wherein generating a digital signature request comprises encrypting control information that includes an identification code of the printing device **(column 11, lines 52-61; note that the printer has the appropriate encryption key such that it will not needlessly print out garbled data)**.

(3) regarding claim 5:

Slick et al. further disclose the method of claim 1, wherein generating a signed request comprises generating a signed request that further includes an unencrypted version of the control information (**column 14, lines 43-45; note that the unencrypted version is used to generated the secure client header)** and wherein the other information used in the comparison comprises the unencrypted version of the control information (**500, figure 8, column 14, lines 47-53; note that the unencrypted version is utilized to check the if the print job requires some type of recipient authentication before the print job is to be printed out**).

(4) regarding claim 13:

As shown in figure 10A, Slick et al. discloses means provided on the computer for generating a digital signature by encrypting with a private key control information (**column 1, lines 29-30; note that private key is generally maintained within the printer and in column 2, lines 38-41, it is stated that a key is encrypted within the printer itself. Also, in column 16, lines 39-42, the key used is a digital signature**);

the signed request including the digital signature (**column 16, lines 40-42; note that the key is used to apply a digital signature to the signed hash fields**); decrypting with a public key associated with the private key the digital signature to obtain decrypted control information (**column 1, line 65-column 2, lines 4; note that the validated key gets checked on the public key by performing a hashing algorithm over the key. Also, the network device utilizes a corresponding encryption key of the new encryption keypair to decrypt the encrypted print job**); and means for the printing device for comparing the decrypted control information with other information to determine if they match (**column 11, lines 61-66; note that the encrypted key is checked to match an expected value**), a match indicating that the signed request is valid (**column 2, lines 42-44; note that the key i.e. digital signature as described in column 16, lines 39-42, gets validated**);

Slick et al. disclose all of the subject matter as described as above except for specifically teaching a system for changing a printing mode of *a printing device that is to be used on future print jobs*; the system including a computer and a printing device, the system further comprising: means provided on the computer for generating a signed request independent of a print job that requests changing of the printing mode of the printing device *that will be used for print jobs that are received by the printing device*; means provided for the printing device for validating the signed request; and means provided on the printing device changing the printing mode relative to received signed requests.

However, As shown in figures 4-5, Kurishita et al. disclose a system for changing a printing mode **(column 2, lines 1-9; note that a print method for securely printing print data is disclosed**) of *a printing device that is to be used on future print jobs (***column 2, lines 18-19; note that the method is used to print job or data in a printing device***)*; the system including a computer and a printing device (**104, 401, figure 1**), the system further comprising, the method comprising: means provided on the computer for generating a signed request that requests changing of the printing mode of a printing device **(column 6, lines 11-17; note that there is a generated user information for authenticating the print data. Also, column 5, lines 30-34; note that the printing device receives instruction from the host computer**) *that will be used for print jobs that are received by the printing device (***column 6, lines 4-8; note that the user goes to the printer and operated the input operation or the printing operation***)*; providing the signed request to the printing device (**column 6, lines 11-17; note that user inputs user name as a signed request**); means provided for the printing device for validating the signed request **(column 6, lines 18-25; note that based upon the requestors input i.e. user name selected, the user gets validated or authorized**); and means provided on the printing device changing the printing mode relative to received signed requests **(column 6, lines 26-32; note that if the data entered in valid, the print data stored is transmitted to be printed or executed**).

Slick et al. and Kurishita et al. are combinable because they are from the same field of endeavor i.e. network printing. At the time of the invention, it would have been obvious to a person of ordinary skilled in the art to have a system for changing a printing

mode of *a printing device that is to be used on future print jobs*; the system including a computer and a printing device, the system further comprising: means provided on the computer for generating a signed request independent of a print job that requests changing of the printing mode of the printing device *that will be used for print jobs that are received by the printing device*; means provided for the printing device for validating the signed request; and means provided on the printing device changing the printing mode relative to received signed requests. The suggestion/motivation for doing so would have been to have a reliable and secure print system such that a user having issues a print request can reliably obtain printouts while observing secrecy (column 1, lines 7-10). Therefore, it would have been obvious to combine Slick et al. and Kurishita et al. to obtain the invention as specified in claim 13.

(5) regarding claim 15:

Slick et al. further disclose the method of claim 13, wherein generating a digital signature request comprises encrypting control information that includes an identification code of the printing device (**column 11, lines 52-61; note that the printer has the appropriate encryption key such that it will not needlessly print out garbled data**).

(6) regarding claim 21:

Slick et al. further disclose the method of claim 20, wherein generating a digital signature request comprises encrypting control information that includes an

identification code of the printing device (**column 11, lines 52-61; note that the printer has the appropriate encryption key such that it will not needlessly print out garbled data**).

(7) regarding claim 22:

Slick et al. further disclose the method of claim 20, wherein generating a signed request comprises generating a signed request that further includes an unencrypted version of the control information (**column 14, lines 43-45; note that the unencrypted version is used to generated the secure client header**) and wherein the other information used in the comparison comprises the unencrypted version of the control information (**500, figure 8, column 14, lines 47-53; note that the unencrypted version is utilized to check the if the print job requires some type of recipient authentication before the print job is to be printed out**).

(8) regarding claim 36:

Slick et al. disclose all of the subject matter as described as above except for specifically teaching wherein the identification code is a serial number or a media-access control (MAC) address of the printing device.

However, Kurishita et al. disclose wherein the identification code is a serial number or a media-access control (MAC) address of the printing device (**column 4, lines 28-35; note that the virtual printer is selected as the security printer based on the name stored in the RAM or external memory**).

Slick et al. and Kurishita et al. are combinable because they are from the same field of endeavor i.e. network printing. At the time of the invention, it would have been obvious to a person of ordinary skilled in the art to wherein the identification code is a serial number or a media-access control (MAC) address of the printing device. The suggestion/motivation for doing so would have been to have a reliable and secure print system such that a user having issues a print request can reliably obtain printouts while observing secrecy (column 1, lines 7-10). Therefore, it would have been obvious to combine Slick et al. and Kurishita et al. to obtain the invention as specified in claim 36.

(9) regarding claim 37:

Slick et al. disclose all of the subject matter as described as above except for specifically teaching wherein generating a digital signature comprises encrypting print information that further includes an identity of service provider that controls the printing device, identity of a client wishing to use the printing device, or an indication as to when the requested mode is to expire.

However, Kurishita et al. disclose wherein generating a digital signature comprises encrypting print information that further includes an identity of service provider that controls the printing device, identity of a client wishing to use the printing device, or an indication as to when the requested mode is to expire (**column 10, lines 17-24; note that user's information is selected as a signed request**).

Slick et al. and Kurishita et al. are combinable because they are from the same field of endeavor i.e. network printing. At the time of the invention, it would have been

obvious to a person of ordinary skilled in the art to wherein generating a digital signature comprises encrypting print information that further includes an identity of service provider that controls the printing device, identity of a client wishing to use the printing device, or an indication as to when the requested mode is to expire. The suggestion/motivation for doing so would have been to have a reliable and secure print system such that a user having issues a print request can reliably obtain printouts while observing secrecy (column 1, lines 7-10). Therefore, it would have been obvious to combine Slick et al. and Kurishita et al. to obtain the invention as specified in claim 37.

6. Claim 20 recites identical feature as claim 13, except claim 20 is a computer-readable media. Thus arguments similar to that presented above for claim 13 are equally applicable to claim 20.

7. Claims 11-12 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slick et al. (US Patent Number 7,111,322 B2) and Kurishita et al. (US Patent Number 7,100,198 B2) as applied to claim 1 above and further in view of Kawamoto et al. (US Patent Number 6,120,197).

(1) regarding claims 11 and 19:

Kurishita et al. and Slick et al. disclose all of the subject matter as described as above except for specifically teaching, wherein enabling or disabling the printing mode comprises enabling or disabling reduced-toner printing.

However, Kawamoto et al. teach wherein enabling or disabling the printing mode comprises enabling or disabling reduced-toner printing (**column 11, lines 60-65; note that the color processing mode can be changed every page in the printer so that the toner can be reduced and a print throughput can be improved**).

Kurishita et al., Slick et al. and Kawamoto et al. are combinable because they are from the same field of endeavor which is network printing method. At the time of the invention, it would have been obvious to a person of ordinary skilled in the art wherein enabling or disabling the printing mode comprises enabling or disabling reduced-toner printing. The suggestion/motivation for doing so would have been in order to save time it takes to change different modes (column 1, lines 47-50). Also, such method also improves print quality (column 1, lines 44-47). Therefore, it would have been obvious to combine Kurishita et al. and Slick et al. with Kawamoto et al. to obtain the invention as specified in claim 11.

(2) regarding claim 12:

Kurishita et al. and Slick et al. disclose all of the subject matter as described as above except for specifically teaching, wherein enabling or disabling the printing mode comprises enabling or disabling CMYK printing.

However, Kawamoto et al. teach wherein enabling or disabling the printing mode comprises enabling or disabling CMYK printing (**column 2, lines 10-15; note that the color processing mode is determined by a page unit of the print data**).

Kurishita et al., Slick et al. and Kawamoto et al. are combinable because they are from the same field of endeavor which is network printing method. At the time of the invention, it would have been obvious to a person of ordinary skilled in the art wherein enabling or disabling the printing mode comprises enabling or disabling CMYK printing. The suggestion/motivation for doing so would have been in order to save time it takes to change different modes (column 1, lines 47-50). Also, such method also improves print quality (column 1, lines 44-47). Therefore, it would have been obvious to combine Kurishita et al. and Slick et al. with Kawamoto et al. to obtain the invention as specified in claim 12.

Conclusion

8. Any inquiry concerning this communication or earlier communication from the examiner should be directed to Hilina Kassa whose telephone number is (571) 270-1676.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Moore could be reached at (571) 272- 7437. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about PAIR system, see http://pari-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Hilina S Kassa/
Examiner, Art Unit 2625
October 27, 2008

/David K Moore/
Supervisory Patent Examiner, Art Unit 2625